

# BOUNDS AND CONSTRUCTIONS FOR $\bar{3}$ -SEPARABLE CODES WITH LENGTH 3

MINQUAN CHENG, JING JIANG, HAIYAN LI, YING MIAO, AND XIAOHU TANG

**ABSTRACT.** Separable codes were introduced to provide protection against illegal redistribution of copyrighted multimedia material. Let  $\mathcal{C}$  be a code of length  $n$  over an alphabet of  $q$  letters. The descendant code  $\text{desc}(\mathcal{C}_0)$  of  $\mathcal{C}_0 = \{\mathbf{c}_1, \mathbf{c}_2, \dots, \mathbf{c}_t\} \subseteq \mathcal{C}$  is defined to be the set of words  $\mathbf{x} = (x_1, x_2, \dots, x_n)^T$  such that  $x_i \in \{c_{1,i}, c_{2,i}, \dots, c_{t,i}\}$  for all  $i = 1, \dots, n$ , where  $\mathbf{c}_j = (c_{j,1}, c_{j,2}, \dots, c_{j,n})^T$ .  $\mathcal{C}$  is a  $\bar{t}$ -separable code if for any two distinct  $\mathcal{C}_1, \mathcal{C}_2 \subseteq \mathcal{C}$  with  $|\mathcal{C}_1| \leq t$ ,  $|\mathcal{C}_2| \leq t$ , we always have  $\text{desc}(\mathcal{C}_1) \neq \text{desc}(\mathcal{C}_2)$ . Let  $M(\bar{t}, n, q)$  denote the maximal possible size of such a separable code. In this paper, an upper bound on  $M(\bar{3}, 3, q)$  is derived by considering an optimization problem related to a partial Latin square, and then two constructions for  $\bar{3}$ -SC(3,  $M, q$ )s are provided by means of perfect hash families and Steiner triple systems.

## 1. INTRODUCTION

Separable codes can be used to construct multimedia fingerprinting codes which can effectively trace and even identify the sources of pirate copies of copyrighted multimedia data, see, *e.g.*, [8, 13]. They are of interest in combinatorics and can be also used to study the classic digital fingerprinting codes such as identifiable parent property (IPP) codes [9, 10], frameproof codes (FPCs) [2, 5], perfect hash families (PHFs) [11] and so on. Cheng and Miao [8] pointed out that IPP codes, FPCs, PHFs and some other structures in digital fingerprinting are in fact examples of separable codes with additional properties.

Let  $n, M$  and  $q$  be positive integers, and  $Q$  be an alphabet with  $|Q| = q$ . A set  $\mathcal{C} = \{\mathbf{c}_1, \mathbf{c}_2, \dots, \mathbf{c}_M\} \subseteq Q^n$  is called an  $(n, M, q)$  code and each  $\mathbf{c}_i$  is called a codeword. Without loss of generality, we may assume  $Q = \{0, 1, \dots, q-1\}$ . When  $Q = \{0, 1\}$ , we also use the word “binary”. Given an  $(n, M, q)$  code, its incidence matrix is the  $n \times M$  matrix on  $Q$  in which the columns are the  $M$  codewords in  $\mathcal{C}$ . We do not distinguish an  $(n, M, q)$  code and its incidence matrix unless otherwise stated.

For any subset of codewords  $\mathcal{C}_0 \subseteq \mathcal{C}$ , we define the set of  $i$ th coordinates of  $\mathcal{C}_0$  as

$$\mathcal{C}_0(i) = \{c_i \in Q \mid \mathbf{c} = (c_1, c_2, \dots, c_n)^T \in \mathcal{C}_0\}, \quad 1 \leq i \leq n,$$

---

*Date:* Received: date / Accepted: date.

2010 *Mathematics Subject Classification.* 94A62, 94B25, 05B15, 05B30.

*Key words and phrases.* Multimedia fingerprinting, separable code, partial Latin square, perfect hash family, Steiner triple system.

Cheng is supported in part by NSFC (No.11301098), Guangxi Natural Science Foundations (No.2013GXNSFCA019001 and 2014GXNSFDA118001), and Foundation of Guangxi Education Department (No.2013YB039). Jiang is supported by the Guangxi Natural Science Foundation (No.2012GXNSFGA060004) and Guangxi “Bagui Scholar” Teams for Innovation and Research. Miao is supported by JSPS Grant-in-Aid for Scientific Research (C) (No.15K04974).

and the descendant code of  $\mathcal{C}_0$  as

$$\text{desc}(\mathcal{C}_0) = \{\mathbf{x} = (x_1, x_2, \dots, x_n)^T \in Q^n \mid x_i \in \mathcal{C}_0(i), 1 \leq i \leq n\},$$

that is,

$$\text{desc}(\mathcal{C}_0) = \mathcal{C}_0(1) \times \mathcal{C}_0(2) \times \dots \times \mathcal{C}_0(n).$$

**Definition 1.1.** Let  $\mathcal{C}$  be an  $(n, M, q)$  code and  $t \geq 2$  be an integer.

- (1)  $\mathcal{C}$  is a  $t$ -separable code, or  $t$ -SC( $n, M, q$ ), if for any  $\mathcal{C}_1, \mathcal{C}_2 \subseteq \mathcal{C}$  such that  $|\mathcal{C}_1| = |\mathcal{C}_2| = t$  and  $\mathcal{C}_1 \neq \mathcal{C}_2$ , we have  $\text{desc}(\mathcal{C}_1) \neq \text{desc}(\mathcal{C}_2)$ , that is, there is at least one coordinate  $i$ ,  $1 \leq i \leq n$ , such that  $\mathcal{C}_1(i) \neq \mathcal{C}_2(i)$ .
- (2)  $\mathcal{C}$  is a  $\bar{t}$ -separable code, or  $\bar{t}$ -SC( $n, M, q$ ), if for any  $\mathcal{C}_1, \mathcal{C}_2 \subseteq \mathcal{C}$  such that  $|\mathcal{C}_1| \leq t$ ,  $|\mathcal{C}_2| \leq t$  and  $\mathcal{C}_1 \neq \mathcal{C}_2$ , we have  $\text{desc}(\mathcal{C}_1) \neq \text{desc}(\mathcal{C}_2)$ , that is, there is at least one coordinate  $i$ ,  $1 \leq i \leq n$ , such that  $\mathcal{C}_1(i) \neq \mathcal{C}_2(i)$ .
- (3)  $\mathcal{C}$  is a  $t$ -frameproof code, or  $t$ -FPC( $n, M, q$ ), if for any  $\mathcal{C}' \subseteq \mathcal{C}$  such that  $|\mathcal{C}'| \leq t$ , we have that  $\text{desc}(\mathcal{C}') \cap \mathcal{C} = \mathcal{C}'$ , that is, for any  $\mathbf{c} = (c_1, \dots, c_n)^T \in \mathcal{C} \setminus \mathcal{C}'$ , there is at least one coordinate  $i$ ,  $1 \leq i \leq n$ , such that  $c_i \notin \mathcal{C}'(i)$ .

Cheng et al. [7, 8] established the following relationships between frameproof codes and separable codes.

**Lemma 1.2.** ([8]) A  $t$ -FPC( $n, M, q$ ) is also a  $\bar{t}$ -SC( $n, M, q$ ).

**Theorem 1.3.** ([7]) An  $(n, M, q)$  code  $\mathcal{C}$  is a  $\bar{t}$ -SC( $n, M, q$ ) if and only if  $\mathcal{C}$  is a  $(t-1)$ -FPC( $n, M, q$ ) and a  $t$ -SC( $n, M, q$ ).

Since the parameter  $M$  of a  $\bar{t}$ -SC( $n, M, q$ ) corresponds to the number of fingerprints assigned to authorized users who purchased the right to access the copyrighted multimedia data, we should try to construct separable codes with  $M$  as large as possible, given length  $n$ . Let  $M(\bar{t}, n, q) = \max\{M \mid \text{there exists a } \bar{t}\text{-SC}(n, M, q)\}$ . A  $\bar{t}$ -SC( $n, M, q$ ) is said to be optimal if  $M = M(\bar{t}, n, q)$ . Similarly, a  $t$ -FPC( $n, M, q$ ) is optimal if  $M$  is the largest possible value given  $n$ ,  $q$  and  $t$ . From the relationship above, Cheng et al. obtained the following upper bound on  $M(\bar{t}, n, q)$ .

**Theorem 1.4.** ([7]) Let  $n, q$  and  $t$  be positive integers such that  $t \geq 3$  and  $n \geq 2$ , and let  $r \in \{0, 1, \dots, t-2\}$  be the remainder of  $n$  on division by  $t-1$ . If  $M(\bar{t}, n, q) > q$ , then

$$M(\bar{t}, n, q) \leq \max\{q^{\lceil n/(t-1) \rceil}, r(q^{\lceil n/(t-1) \rceil} - 1) + (t-1-r)(q^{\lceil n/(t-1) \rceil} - 1)\}.$$

Bazrafshan and Trung showed the following results.

**Lemma 1.5.** ([1]) For any positive integers  $t$  and  $q \geq 2$ , the following code is an optimal  $t$ -FPC( $n, n(q-1), q$ ) when  $2 \leq n \leq t$ .

$$\begin{pmatrix} 1 & 2 & \dots & q-1 & 0 & 0 & \dots & 0 & \dots & 0 & 0 & \dots & 0 \\ 0 & 0 & \dots & 0 & 1 & 2 & \dots & q-1 & \dots & 0 & 0 & \dots & 0 \\ & & \vdots & & & & \vdots & & \ddots & & & \vdots & \\ 0 & 0 & \dots & 0 & 0 & 0 & \dots & 0 & \dots & 1 & 2 & \dots & q-1 \end{pmatrix}$$

**Lemma 1.6.** ([1]) For a  $t$ -FPC( $n, M, q$ ) with  $n = 1 + t$  we have

- (i)  $M \leq q^2$ , if  $n \leq q$ ,
- (ii)  $M \leq nq$ , if  $n > q$ .

According to Theorem 1.3 and Lemmas 1.2, 1.5, 1.6, the following corollaries can be obtained.

**Corollary 1.7.** For any positive integers  $t$  and  $q \geq 2$ , there always exists an optimal  $\bar{t}$ -SC( $n, n(q-1), q$ ) when  $2 \leq n < t$ .

**Corollary 1.8.** In a  $\bar{t}$ -SC( $n, M, q$ ) with  $n = t$  we have

- (i)  $M \leq q^2$ , if  $n \leq q$ ,
- (ii)  $M \leq nq$ , if  $n > q$ .

Using random choice with expurgation, Blackburn [4] showed the following result.

**Theorem 1.9.** ([4]) Let  $n$  and  $t$  be fixed integers such that  $n \geq 2$  and  $t \geq 3$ . There exists a positive constant  $\kappa$ , depending only on  $n$  and  $t$ , so that there is a  $q$ -ary  $\bar{t}$ -separable code of length  $n$  with at least  $\kappa q^{n/(t-1)}$  codewords for all sufficiently large integers  $q$ .

**Corollary 1.10.** There exists a positive constant  $\kappa$ , depending only on  $n$  and  $t$ , so that  $M(\bar{t}, n, q) \geq \kappa q^{n/(t-1)}$  for all sufficiently large integers  $q$ .

Cheng and Miao [8] showed that long-length separable codes can be constructed by concatenating short-length separable codes. This stimulates the investigation of separable codes with short length  $n = 2, 3$ . When  $n = 2, 3$ , upper bounds on  $M(\bar{2}, n, q)$  were derived, and several infinite series of optimal  $\bar{2}$ -SC( $n, M, q$ )s were constructed in [6, 7]. When  $t \geq 3$ , the structure of  $\bar{t}$ -SCs becomes more complex so that little is known about  $\bar{t}$ -SCs for  $t \geq 3$ .

In this paper, we mainly study  $\bar{3}$ -SCs. When  $n = 2$ , by Corollary 1.7, we know that for any integer  $q \geq 2$ , there always exists an optimal  $\bar{3}$ -SC( $2, 2(q-1), q$ ). When  $n = 3$  and  $q = 2$ , an exhaustive computer search shows that  $\mathcal{C} = \{(1, 0, 0)^T, (0, 1, 0)^T, (0, 0, 1)^T\}$  is an optimal  $\bar{3}$ -SC( $3, 3, 2$ ). When  $q > 2$ , we have  $M(\bar{3}, 3, q) \leq q^2$  by Corollary 1.8. However, this upper bound is not tight. In the following sections, we will first derive a new upper bound  $M(\bar{3}, 3, q) \leq \lfloor \frac{3q^2}{4} \rfloor$  by considering an optimization problem related to a partial Latin square. Two constructions for  $\bar{3}$ -SC( $3, M, q$ )s will be then provided by means of perfect hash families and Steiner triple systems. The first one shows that  $\bar{3}$ -SC( $3, M, q$ )s with  $M = O(q^{3/2})$  codewords, the lower bound provided by Blackburn (Corollary 1.10) using a probabilistic proof, can be constructed explicitly for all integers  $q$ . The second one shows that  $\bar{3}$ -SC( $3, M, q$ )s with  $M = O(q^2)$  codewords do exist.

## 2. FORBIDDEN CONFIGURATIONS

In this section, we first show that a  $\bar{3}$ -separable code,  $\mathcal{C}$ , cannot contain certain subcodes, that is, there are certain forbidden configurations in  $\mathcal{C}$ . Then we use these forbidden configurations, together with the 2-frameproof code property, to give a necessary and sufficient condition for a  $(3, M, q)$  code to be a  $\bar{3}$ -SC( $3, M, q$ ).

For any  $(3, M, q)$  code  $\mathcal{C}$  defined on  $Q$ , we define two shortened codes  $A_i^{(1)}$  and  $A_{i,k}^{(1,2)}$  for  $i, k \in Q$  as

$$A_i^{(1)} = \{(c_2, c_3) \mid (i, c_2, c_3)^T \in \mathcal{C}\} \text{ and } A_{i,k}^{(1,2)} = \{c_3 \mid (i, k, c_3)^T \in \mathcal{C}\},$$

respectively. Obviously,  $A_i^{(1)} \subseteq Q^2$  and  $A_{i,k}^{(1,2)} \subseteq Q$  hold for any  $i, k \in Q$ , and

$$\sum_{i \in Q} |A_i^{(1)}| = \sum_{i \in Q} \sum_{k \in Q} |A_{i,k}^{(1,2)}| = M.$$

Similarly,  $A_i^{(2)}$  and  $A_i^{(3)}$  for  $i \in Q$  can be defined. Cheng et al. [7] obtained the following result.

**Lemma 2.1.** [7] If  $\mathcal{C}$  is a  $\bar{t}$ -SC( $n, M, q$ ), then  $|A_i^{(j)} \cap A_{i'}^{(j)}| \leq 1$  holds for any distinct  $i, i' \in Q$  and  $j = 1, 2, \dots, n$ .

From the notions above and the definition of an FPC, the following Lemma 2.2 can be obtained.

**Lemma 2.2.** A  $(3, M, q)$  code is a 2-FPC( $3, M, q$ ) if and only if  $|A_i^{(j)} \cap A_{i'}^{(j)}| \leq 1$  holds for any  $j \in \{1, 2, 3\}$  and distinct  $i, i' \in Q$ , where if  $|A_i^{(j)} \cap A_{i'}^{(j)}| = 1$ , then  $|A_i^{(j)}| = |A_{i'}^{(j)}| = 1$ .

**Proof:** Let  $\mathcal{C}$  be a  $(3, M, q)$  code. We first suppose that  $\mathcal{C}$  is a 2-FPC( $3, M, q$ ). According to Lemma 1.2,  $\mathcal{C}$  is a  $\bar{2}$ -SC( $3, M, q$ ). So for any  $j \in \{1, 2, 3\}$  and distinct  $i, i' \in Q$ ,  $|A_i^{(j)} \cap A_{i'}^{(j)}| \leq 1$  holds by Lemma 2.1. When  $|A_i^{(j)} \cap A_{i'}^{(j)}| = 1$ , without loss of generality, we may assume that  $j = 1$  and  $\{\mathbf{a}\} = A_i^{(1)} \cap A_{i'}^{(1)}$ . If there is another element  $\mathbf{b} \in A_i^{(1)}$ , then we have  $(i, \mathbf{a})^T, (i, \mathbf{b})^T, (i', \mathbf{a})^T \in \mathcal{C}$ ,  $\{(i', \mathbf{a})^T, (i, \mathbf{b})^T\} \cap \{(i, \mathbf{a})^T\} = \emptyset$ , and  $(i, \mathbf{a})^T \in \text{desc}(\{(i', \mathbf{a})^T, (i, \mathbf{b})^T\}) \cap \mathcal{C}$ . This contradicts the definition of a frameproof code. So  $|A_i^{(1)}| = 1$  holds. Similarly,  $|A_{i'}^{(1)}| = 1$  can be proved.

Conversely, if  $\mathcal{C}$  is not a 2-FPC( $3, M, q$ ), then there exist three distinct codewords  $\mathbf{a} = (a_1, a_2, a_3)^T$ ,  $\mathbf{b} = (b_1, b_2, b_3)^T$ ,  $\mathbf{c} = (c_1, c_2, c_3)^T \in \mathcal{C}$ , such that  $\mathbf{c} \in \text{desc}(\{\mathbf{a}, \mathbf{b}\})$ . Since the codeword length equals 3, there exists at least one codeword, say  $\mathbf{a}$ , such that it contains two same coordinates as  $\mathbf{c}$ , say  $a_2 = c_2$  and  $a_3 = c_3$ . Since  $\mathbf{c} \in \text{desc}(\{\mathbf{a}, \mathbf{b}\})$ , then  $b_1 = c_1$ . That is,  $\mathbf{c} = (b_1, a_2, a_3)^T$ . Obviously,  $|A_{a_1}^{(1)} \cap A_{b_1}^{(1)}| \geq 1$  and  $|A_{b_1}^{(1)}| \geq 2$ , which contradict our assumption.  $\square$

Now, let us turn our attention to  $\bar{3}$ -SC( $3, M, q$ )s. For any  $\bar{3}$ -SC( $3, M, q$ ),  $\mathcal{C}$ , it can be checked that there is no subcode  $\Delta_1 \subseteq \mathcal{C}$  described in (1).

$$\Delta_1 = \begin{pmatrix} a & a & b & b \\ e & f & g & e \\ c & d & c & d \end{pmatrix}, \quad \Delta_2 = \begin{pmatrix} a & a & b & b \\ c & d & c & d \\ e & f & g & e \end{pmatrix}, \quad \Delta_3 = \begin{pmatrix} e & f & g & e \\ a & a & b & b \\ c & d & c & d \end{pmatrix}. \quad (1)$$

The reason is as follows. If  $\mathcal{C}$  contains the configuration  $\Delta_1$ , then since  $\mathcal{C}$  is also a 2-FPC( $3, M, q$ ) by Theorem 1.3, we should have  $a \neq b$ ,  $c \neq d$  and  $e \notin \{f, g\}$ . However, in this case,  $\{(a, e, c)^T, (a, f, d)^T, (b, g, c)^T\} \neq \{(a, f, d)^T, (b, g, c)^T, (b, e, d)^T\}$ , but  $\text{desc}(\{(a, e, c)^T, (a, f, d)^T, (b, g, c)^T\}) = \text{desc}(\{(a, f, d)^T, (b, g, c)^T, (b, e, d)^T\})$ , a contradiction to the definition of a  $\bar{3}$ -SC. We call such  $\Delta_1$  a *forbidden configuration* of  $\mathcal{C}$ . Given

a subcode  $\mathcal{C}' \subseteq \mathcal{C}$ , conjugates of  $\mathcal{C}'$  are subsets of  $Q^3$  defined by changing any two coordinates of  $\mathcal{C}'$ . Clearly,  $\triangle_1$  and its conjugates in (1) are forbidden configurations of  $\mathcal{C}$ .

It is easy to check that the following  $\nabla$  is also a forbidden configuration of  $\mathcal{C}$ , where  $|\{a_i, b_i, c_i\}| = 3$ ,  $i = 1, 2, 3$ .

$$\nabla = \begin{pmatrix} a_1 & b_1 & c_1 & a_1 & b_1 & c_1 \\ a_2 & b_2 & c_2 & b_2 & c_2 & a_2 \\ a_3 & b_3 & c_3 & c_3 & a_3 & b_3 \end{pmatrix} \quad (2)$$

**Theorem 2.3.** A  $(3, M, q)$  code  $\mathcal{C}$  is a  $\overline{3}$ -SC $(3, M, q)$  if and only if it satisfies the following conditions:

- (i)  $\mathcal{C}$  is a 2-FPC $(3, M, q)$ ;
- (ii) Configurations in (1) and (2) are all the forbidden configurations of  $\mathcal{C}$ .

The proof of Theorem 2.3 is included in Appendix.

### 3. AN UPPER BOUND

As we said at the end of Section 1, when  $n = 3$  and  $q > 2$ , we have an upper bound  $M(\overline{3}, 3, q) \leq q^2$ . In this section, we are going to derive a new upper bound  $M(\overline{3}, 3, q) \leq \lfloor \frac{3q^2}{4} \rfloor$  by exploiting the two conditions in Theorem 2.3.

Given a  $\overline{3}$ -SC $(3, M, q)$ ,  $\mathcal{C}$ , defined on  $Q = \{0, 1, \dots, q-1\}$ , the following  $q \times q$  array can be obtained, where each entry is a subset of  $Q$ .

$$\mathfrak{A} = \begin{pmatrix} \mathcal{A}_{0,0}^{(1,2)} & \dots & \mathcal{A}_{0,q-1}^{(1,2)} \\ \mathcal{A}_{1,0}^{(1,2)} & \dots & \mathcal{A}_{1,q-1}^{(1,2)} \\ \dots & \dots & \dots \\ \mathcal{A}_{q-1,0}^{(1,2)} & \dots & \mathcal{A}_{q-1,q-1}^{(1,2)} \end{pmatrix}$$

By Theorem 2.3,  $\mathcal{C}$  is also a 2-FPC $(3, M, q)$ . Then it can be easily checked that  $\mathfrak{A}$  has the following properties.

- (I) P<sub>1.1</sub>: If  $|\mathcal{A}_{i,j}^{(1,2)}| \geq 2$ , then  $\mathcal{A}_{i,j}^{(1,2)} \cap \mathcal{A}_{i',j'}^{(1,2)} = \emptyset$  holds for any  $(i', j') \in Q^2 \setminus \{(i, j)\}$ ;
- P<sub>1.2</sub>: If  $|\mathcal{A}_{i,j}^{(1,2)} \cap \mathcal{A}_{i',j'}^{(1,2)}| = 1$  with  $j \neq j'$ , then  $\mathcal{A}_{i',j}^{(1,2)} = \mathcal{A}_{i',j'}^{(1,2)} = \emptyset$  holds for any  $i' \in Q \setminus \{i\}$ ;
- P<sub>1.3</sub>: If  $|\mathcal{A}_{i,j}^{(1,2)} \cap \mathcal{A}_{i',j}^{(1,2)}| = 1$  with  $i \neq i'$ , then  $\mathcal{A}_{i,j}^{(1,2)} = \mathcal{A}_{i',j}^{(1,2)} = \emptyset$  holds for any  $j' \in Q \setminus \{j\}$ .

Again by Theorem 2.3, configuration  $\triangle_2$  is a forbidden configuration of  $\mathcal{C}$ . Then it is easily seen that  $\mathfrak{A}$  has the following property.

- (II) P<sub>2</sub>: If  $|\mathcal{A}_{i,j}^{(1,2)} \cap \mathcal{A}_{i',j'}^{(1,2)}| = 1$  with  $i \neq i'$ ,  $j \neq j'$ , then  $\mathcal{A}_{i',j}^{(1,2)} = \emptyset$  or  $\mathcal{A}_{i,j'}^{(1,2)} = \emptyset$  holds.

From array  $\mathfrak{A}$ , we can define a related array  $\mathbb{B} = (b_{i,j})$  in the following way:

$$b_{i,j} = \begin{cases} a_{i,j} & \text{if } \mathcal{A}_{i,j}^{(1,2)} = \{a_{i,j}\}, \\ \star & \text{if } 2 \leq |\mathcal{A}_{i,j}^{(1,2)}|, \\ \times & \text{if } \mathcal{A}_{i,j}^{(1,2)} = \emptyset. \end{cases}$$

Let  $\mu_i = |\{j \mid |\mathcal{A}_{i,j}^{(1,2)}| \geq 2, j \in Q\}|$  be the number of sets  $\mathcal{A}_{i,j}^{(1,2)}$  with  $|\mathcal{A}_{i,j}^{(1,2)}| \geq 2$  in the  $i$ th row of  $\mathfrak{A}$ , namely, the number of “ $\star$ ” in the  $i$ th row of  $\mathbb{B}$ . Let  $\rho_i = \sum_{j \in Q, 2 \leq |\mathcal{A}_{i,j}^{(1,2)}|} |\mathcal{A}_{i,j}^{(1,2)}|$  be the sum of orders of  $\mathcal{A}_{i,j}^{(1,2)}$  with  $|\mathcal{A}_{i,j}^{(1,2)}| \geq 2$  in the  $i$ th row of  $\mathfrak{A}$ . Then according to P<sub>1.1</sub>, we know that the sum of orders of  $\mathcal{A}_{i,j}^{(1,2)}$  with  $|\mathcal{A}_{i,j}^{(1,2)}| \geq 2$  in  $\mathfrak{A}$  is

$$\sum_{i \in Q} \rho_i = \left| \bigcup_{\substack{i,j \in Q \\ |\mathcal{A}_{i,j}^{(1,2)}| \geq 2}} \mathcal{A}_{i,j}^{(1,2)} \right| = \sum_{\substack{i,j \in Q \\ |\mathcal{A}_{i,j}^{(1,2)}| \geq 2}} |\mathcal{A}_{i,j}^{(1,2)}|.$$

Let  $D_i$  be the set of elements of  $Q$  occurring at least twice in the  $i$ th row of  $\mathbb{B}$ . Let  $m_i$  be the sum of frequencies of elements in  $D_i$  in the  $i$ th row of  $\mathbb{B}$ ,  $m(-i) = \sum_{l \in Q \setminus \{i\}} m_l$  and  $m = \sum_{l \in Q} m_l$ . Let  $B_i$  be the set of elements of  $Q$  occurring exactly once in the  $i$ th row of  $\mathbb{B}$ . Let  $z_{i,j} = |B_i \cap B_j|$ . Clearly,  $z_{i,j} \leq q$ .

Now we consider the total number of distinct elements of  $Q$  in the  $i$ th and  $j$ th rows of  $\mathbb{B}$ . The number of distinct elements of  $Q$  in any  $l$ th row of  $\mathbb{B}$  is  $|B_l| + |D_l|$ . The number of distinct elements of  $Q$  in the  $i$ th and  $j$ th rows of  $\mathbb{B}$  is at least  $|B_i| + |B_j| - |B_i \cap B_j|$ , and from the definition of  $\rho_l$  and property P<sub>1.1</sub>, is at most  $q - \sum_{i \in Q} \rho_i$ . So we have

$$|B_i| + |B_j| - |B_i \cap B_j| \leq q - \sum_{l \in Q} \rho_l.$$

We also consider the number of entries in the  $i$ th and  $j$ th rows of  $\mathbb{B}$ . Clearly, for the  $l$ th row of  $\mathbb{B}$ ,  $m(-l) + \mu_l + m_l + |B_l| \leq q$ , and for the  $i$ th and  $j$ th rows of  $\mathbb{B}$ ,

$$[|B_i| + \mu_i + m(-i) + m_i] + [|B_j| + \mu_j + m(-j) + m_j] + z_{i,j} \leq 2q$$

where the term “ $z_{i,j}$ ” is the number of additional “ $\times$ ” caused by the forbidden configuration  $\triangle_2$ .

We are in a position to derive our new upper bound on  $M(\overline{3}, 3, q)$ .

**Theorem 3.1.**  $M(\overline{3}, 3, q) \leq \lfloor \frac{3q^2}{4} \rfloor$  holds for  $q \geq 4$ .

**Proof:** Let  $\mathcal{C}$  be a  $\overline{3}$ -SC(3,  $M$ ,  $q$ ) defined on  $Q$ . Clearly,  $M = \sum_{i,l \in Q} |\mathcal{A}_{i,l}^{(1,2)}|$ , where  $\sum_{l \in Q} |\mathcal{A}_{i,l}^{(1,2)}| = \rho_i + m_i + |B_i|$ . So our goal is to solve the following optimization problem.

$$\left\{ \begin{array}{ll} \text{Maximize} & \sum_{i \in Q} (\rho_i + m_i + |B_i|) \\ \text{Subject to} & 2m + \mu_i + |B_i| + \mu_j + |B_j| + z_{i,j} \leq 2q \\ & |B_i| + |B_j| - z_{i,j} + \sum_{l \in Q} \rho_l \leq q \\ & i, j \in Q. \end{array} \right.$$

From the constraints above, we have

$$2m + \mu_i + \mu_j + 2(|B_i| + |B_j|) + \sum_{l \in Q} \rho_l \leq 3q.$$

Summarizing the inequality above for all  $i \neq j$ , we have

$$2(q-1) \sum_{l \in Q} |B_l| + (q-1) \sum_{l \in Q} \mu_l + 2m \binom{q}{2} + \binom{q}{2} \sum_{l \in Q} \rho_l \leq 3q \binom{q}{2}.$$

When  $2(q-1) \leq \binom{q}{2}$ , that is,  $q \geq 4$ , we have

$$\begin{aligned} 2(q-1)M &= 2(q-1) \sum_{l \in Q} (|B_l| + m_l + \rho_l) \\ &\leq 2(q-1) \sum_{l \in Q} (|B_l| + m_l) + \binom{q}{2} \sum_{l \in Q} \rho_l \\ &\leq 3q \binom{q}{2} - (q-1) \left( \sum_{l \in Q} \mu_l + (q-2)m \right) \\ &\leq 3q \binom{q}{2}. \end{aligned}$$

This implies  $M \leq \lfloor \frac{3q^2}{4} \rfloor$ .  $\square$

This bound is sharp for some  $q \geq 4$ . In fact, if we can find a  $\overline{3}$ -SC(3,  $M$ ,  $q$ ),  $\mathcal{C}$ , on  $Q$  such that every entry in its corresponding  $\mathfrak{A}$  is a singleton or empty set, no element of  $Q$  appears in any row or column of  $\mathfrak{A}$  more than once, and the number of “ $\times$ ” in each row of  $\mathbb{B}$  is  $\frac{q}{4}$ , then  $M = \frac{3}{4}q^2$ . The following is such an example.

**Example 3.2.** When  $q = 4$ ,  $M(\overline{3}, 3, 4) = 3 \times 4^2/4 = 12$ . Then it can be checked that  $\mathcal{C}_4$  is an optimal  $\overline{3}$ -SC(3, 12, 4). We list it and its related array as follows.

$$\mathcal{C}_4 = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 2 & 2 & 2 & 3 & 3 & 3 \\ 0 & 1 & 2 & 0 & 2 & 3 & 0 & 1 & 3 & 1 & 2 & 3 \\ 0 & 1 & 2 & 1 & 3 & 2 & 3 & 2 & 0 & 3 & 0 & 1 \end{pmatrix}, \quad \mathbb{B}_4 = \begin{pmatrix} 0 & 1 & 2 & \times \\ 1 & \times & 3 & 2 \\ 3 & 2 & \times & 0 \\ \times & 3 & 0 & 1 \end{pmatrix}$$

#### 4. CONSTRUCTIONS

$\mathbb{B}_4$  in Example 3.2 can be regarded as a partial Latin square of order 4, which corresponds to an optimal  $\overline{3}$ -SC(3, 12, 4). In this section, we use partial Latin squares to construct  $\overline{3}$ -SC(3,  $M$ ,  $q$ )s. The definition of a partial Latin square is given below.

**Definition 4.1.** A *partial Latin square*  $\mathbb{P}$  of order  $q$  is a  $q \times q$  array with entries chosen from a  $q$ -set  $Q$  in such a way that each element of  $Q$  occurs at most once in each row and at most once in each column of the array. If all the cells of the array are filled then the partial Latin square is termed a Latin square.

For ease of exposition, a partial Latin square  $\mathbb{P}$  will be represented by a set of ordered triples  $\{(i, j, P_{ij}) \mid \text{element } P_{ij} \text{ occurs in cell } (i, j) \text{ of the array}\}$ .

**Lemma 4.2.** For any partial Latin square  $\mathbb{P}$ , its associated code  $\mathcal{C} = \{\mathbf{c} \mid \mathbf{c} = (i, j, P_{ij})^T \mid (i, j, P_{ij}) \in \mathbb{P}\}$  is a 2-FPC.

**Proof:** Suppose  $\mathcal{C}$  is not a 2-FPC. Then there exist  $\mathcal{C}' = \{\mathbf{a}, \mathbf{b}\} \subseteq \mathcal{C}$  and  $\mathbf{c} = (c_1, c_2, c_3)^T \in \mathcal{C} \setminus \mathcal{C}'$  such that  $\mathbf{c} \in \text{desc}(\mathcal{C}')$ . This implies that there exists a codeword, say  $\mathbf{b} = (b_1, b_2, b_3)^T \in \mathcal{C}'$ , such that there are at least two coordinates  $i, j \in \{1, 2, 3\}$  satisfying  $b_i = c_i$  and  $b_j = c_j$ . If  $(i, j) = (1, 2)$ , then  $\{(c_1, c_2, c_3), (c_1, c_2, b_3)\} \subseteq \mathbb{P}$ , that is, cell  $(c_1, c_2)$  contains both  $c_3$  and  $b_3$ , a contradiction to the definition of a partial Latin square. Similarly, it is readily checked that neither  $(i, j) = (1, 3)$  nor  $(2, 3)$  is possible. The proof is then completed.  $\square$

In the following subsections, we first construct partial Latin squares by means of perfect hash families and Steiner triple systems, respectively, and then show that the associated codes of these partial Latin squares do not contain the forbidden configurations (1) and (2). According to Theorem 2.3, these associated codes are  $\bar{3}\text{-SC}(3, M, q)$ s.

**4.1. Constructions via perfect hash families.** Let  $f$  be a function from a set  $X$  to a set  $Y$ . We say that  $f$  separates a subset  $T \subseteq X$  if  $f$  is injective when  $f$  is restricted to  $T$ ; otherwise we say that  $f$  reduces  $T$ . Let  $M, q, t$  be integers such that  $M \geq q \geq t \geq 2$ . Suppose  $|X| = M$  and  $|Y| = q$ . A set  $\mathcal{F}$  of functions from  $X$  to  $Y$  with  $|\mathcal{F}| = n$  is an  $(n; M, q, t)$ -perfect hash family if for all  $T \subseteq X$  with  $|T| = t$ , there exists at least one  $f \in \mathcal{F}$  such that  $f$  separates  $T$ . We use the notation  $\text{PHF}(n; M, q, t)$  for an  $(n; M, q, t)$ -perfect hash family. A  $\text{PHF}(n; M, q, t)$  can be depicted as an  $n \times M$  array in which the columns are labeled by the elements  $j \in X$ , the rows by the functions  $f_i \in \mathcal{F}$ , and the  $(i, j)$ -entry of the array is the value  $f_i(j)$ . Thus, a  $\text{PHF}(n; M, q, t)$  is equivalent to an  $n \times M$  array with entries from a set of  $q$  symbols such that every  $n \times t$  subarray contains at least one row having distinct symbols. A perfect hash family is optimal if  $M$  is the largest possible value given  $n, q$  and  $t$ .

Given a  $\text{PHF}(n; M, q, t)$ ,  $\mathcal{F} = \{f_1, f_2, \dots, f_n\}$ , we can derive an associated code  $\mathcal{C}$  in an obvious way: associate each  $x \in X$  with the codeword  $(f_1(x), f_2(x), \dots, f_n(x))^T$ . Staddon et al. [10] observed that the associated code of a  $\text{PHF}(n; M, q, t)$  is a  $(t-1)$ -FPC( $n, M, q$ ). However, we should note that the associated codes of a  $\text{PHF}(n; M, q, t)$  is not always a  $\bar{t}\text{-SC}(n, M, q)$ . In fact, we can easily check that  $\nabla$  in (2), a forbidden configuration of  $\bar{3}\text{-SC}(3, M, q)$ , is a  $\text{PHF}(3; 6, q, 3)$ .

In this subsection, we will first show that a special optimal  $\text{PHF}(3; r^3, r^2, 3)$  in [3] is in fact also a  $\bar{3}\text{-SC}(3, r^3, r^2)$ . Based on this  $\text{PHF}(3; r^3, r^2, 3)$ , we then propose a new construction for a  $\bar{3}\text{-SC}(3, r^3 + r^{5/2}, r^2)$  for any even square  $r$ .

Let  $r \geq 2$  be an integer,  $X = Z_r^3$ , and  $Y = Z_{r^2}$ . Define functions  $f_1, f_2, f_3 : X \rightarrow Y$  by

$$f_1((a, b, c)) = ar + b, \quad f_2((a, b, c)) = ar + c \quad \text{and} \quad f_3((a, b, c)) = br + c$$

for all  $a, b, c \in Z_r$ .

**Theorem 4.3.** ([3]) The functions  $f_1, f_2$ , and  $f_3$  defined above form an optimal  $\text{PHF}(3; r^3, r^2, 3)$ .

Let  $\mathcal{C}_1 = \{(f_1((a, b, c)), f_2((a, b, c)), f_3((a, b, c)))^T \mid a, b, c \in Z_r\}$  be the associated code of the above  $\text{PHF}$ . It is not difficult to check that the corresponding  $r^2 \times r^2$  array of  $\mathcal{C}_1$ , in which the rows are labeled by  $f_1((a, b, c))$ , the columns by  $f_2((a, b, c))$ , and  $(f_1((a, b, c)), f_2((a, b, c)))$ -entry is  $f_3((a, b, c))$ , is a partial Latin square. Then Lemma 4.2 shows that  $\mathcal{C}_1$  is a 2-FPC( $3, r^3, r^2$ ). In fact, we can say more about  $\mathcal{C}_1$ .



**Lemma 4.4.**  $\mathcal{C}_1$  is a  $\overline{3}$ -SC( $3, r^3, r^2$ ) for any integer  $r \geq 2$ .

**Proof:** From Theorem 2.3, it is sufficient to prove that forbidden configurations in (1) and (2) cannot occur in  $\mathcal{C}_1$ . It is easy to check that the forbidden configurations in (1) are also forbidden configurations of PHF( $3; r^3, r^2, 3$ ). Now, let us consider the forbidden configuration in (2). Denote a 6-subset of  $\mathcal{C}_1$  by  $C = (\alpha_1, \alpha_2, \dots, \alpha_6)$ , where  $\alpha_i = (a_i r + b_i, a_i r + c_i, b_i r + c_i)^T$ ,  $1 \leq i \leq 6$ . Assume  $C = \nabla$ , then we have

$$\begin{array}{lll} a_1 r + b_1 = a_4 r + b_4 & a_2 r + b_2 = a_5 r + b_5 & a_3 r + b_3 = a_6 r + b_6 \\ a_1 r + c_1 = a_6 r + c_6 & a_2 r + c_2 = a_4 r + c_4 & a_3 r + c_3 = a_5 r + c_5 \\ b_1 r + c_1 = b_5 r + c_5 & b_2 r + c_2 = b_6 r + c_6 & b_3 r + c_3 = b_4 r + c_4 \end{array}$$

which imply  $a_1 = a_2$ ,  $b_1 = b_2$  and  $c_1 = c_2$ , a contradiction to the assumption. Then the proof is completed.  $\square$

From Lemma 4.4, a lower bound can be obtained.

**Corollary 4.5.**  $\lfloor \sqrt{q} \rfloor^3 \leq M(\overline{3}, 3, q)$  holds for  $q \geq 4$ .

Now we illustrate Lemma 4.4 with a small example.

**Example 4.6.** (1) Let  $r = 4$ . Then according to Lemma 4.4, the associated code of  $\mathbb{B}_1$  described below is a  $\overline{3}$ -SC( $3, 64, 16$ ).

$$\mathbb{B}_1 = \begin{pmatrix} A & & & \\ & A & & \\ & & A & \\ & & & A \end{pmatrix}, \text{ where } A = \begin{pmatrix} 0 & 1 & 2 & 3 \\ 4 & 5 & 6 & 7 \\ 8 & 9 & 10 & 11 \\ 12 & 13 & 14 & 15 \end{pmatrix}$$

and other cells of  $\mathbb{B}_1$  are filled with “ $\times$ ”.

(2) Replacing some “ $\times$ ”s in  $\mathbb{B}_1$  by some elements of  $Y = Z_{r^2}$ , we obtain the following array  $\mathbb{B}$ , which is still a partial Latin square. It can be checked that its associated code is a  $\overline{3}$ -SC( $3, 96, 16$ ).

$$\mathbb{B} = \begin{pmatrix} A & A_1 & & & \\ & A & A_2 & & \\ & & A & A_1 & \\ A_2 & & & A & \end{pmatrix}, \text{ where } A_1 = \begin{pmatrix} 10 & 11 \\ 14 & 15 \end{pmatrix}, \quad A_2 = \begin{pmatrix} & 8 & 9 \\ & 12 & 13 \\ 2 & 3 \\ 6 & 7 \end{pmatrix}.$$

Inspired by Example 4.6, for any even square  $r = k^2$ , we define other six functions as follows:

$$\begin{array}{ll} g_1(x, y, z, h) = xk + y + hr, & g_2(x, y, z, h) = xk + z + (h + 1)r, \\ g(x, y) = r - (x + 1)k + y, & g_3(x, y, z, h) = g(x, y)r + g(x, z), \\ g'_2(x, y, z, h) = g(x, z) + (h + 1)r, & g'_3(x, y, z, h) = g(x, y)r + xk + z, \end{array}$$

where all the operations in the above functions are taken in  $Z_{r^2}$ . Using these functions, we further define the following codes.

$$\begin{aligned} \mathcal{C}_2 &= \{(g_1(x, y, z, h), g_2(x, y, z, h), g_3(x, y, z, h))^T \mid x, y, z \in Z_k, h \in Z_r, h \equiv 0 \pmod{2}\}, \\ \mathcal{C}_3 &= \{(g_1(x, y, z, h), g'_2(x, y, z, h), g'_3(x, y, z, h))^T \mid x, y, z \in Z_k, h \in Z_r, h \equiv 1 \pmod{2}\}. \end{aligned}$$

Similar to Lemma 4.4, we have

**Lemma 4.7.** For any even square  $r = k^2$ ,  $\mathcal{C}_2$  is a  $\overline{3}\text{-SC}(3, kr^2/2, r^2)$ , and so is  $\mathcal{C}_3$ .

**Proof:** Let us first consider  $\mathcal{C}_2$ . Let  $X = Z_k^3 \times Z_r$  and  $Y = Z_{r^2}$ . We show that  $\mathcal{F}' = \{g_1, g_2, g_3\}$  forms a PHF( $3; kr^2/2, r^2, 3$ ). It is easy to check that an element  $\mathbf{v} \in X$  is uniquely determined by any two of three images  $g_1(\mathbf{v})$ ,  $g_2(\mathbf{v})$  and  $g_3(\mathbf{v})$ , therefore every 2-subset of  $X$  is reduced by at most one of  $g_1$ ,  $g_2$  and  $g_3$ . Suppose, for a contradiction, that  $\{\mathbf{v}_1 = (x_1, y_1, z_1, h_1), \mathbf{v}_2 = (x_2, y_2, z_2, h_2), \mathbf{v}_3 = (x_3, y_3, z_3, h_3)\} \subseteq X$  is a 3-set that is reduced by all of the functions  $g_1$ ,  $g_2$  and  $g_3$ . Since every 2-set is reduced by at most one of  $g_1$ ,  $g_2$  and  $g_3$  and since every function  $g_i$  must reduce some 2-subset of  $\{\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3\}$ , we may assume without loss of generality that  $g_1(\mathbf{v}_1) = g_1(\mathbf{v}_2)$ ,  $g_2(\mathbf{v}_1) = g_2(\mathbf{v}_3)$  and  $g_3(\mathbf{v}_2) = g_3(\mathbf{v}_3)$ . This implies that  $x_1 = x_2$ ,  $y_1 = y_2$ ,  $z_1 = z_2$  and  $h_1 = h_2$ , a contradiction to the assumption. So  $\mathcal{F}'$  is a 3-PHF( $3; kr^2/2, r^2, 3$ ).

Clearly,  $\mathcal{C}_2$  is the associated code of the perfect hash family  $\mathcal{F}'$ . Similar to the proof of Lemma 4.4, we need only consider the forbidden configuration in (2). Denote a 6-subset of  $\mathcal{C}_2$  by  $C = (\beta_1, \beta_2, \dots, \beta_6)$ , where  $\beta_i = (g_1(x_i, y_i, z_i, h_i), g_2(x_i, y_i, z_i, h_i), g_3(x_i, y_i, z_i, h_i))^T$ ,  $1 \leq i \leq 6$ . Assume  $C = \nabla$ , then we have

$$\begin{aligned} x_1k + y_1 + h_1r &= x_4k + y_4 + h_4r, & x_2k + y_2 + h_2r &= x_5k + y_5 + h_5r, \\ x_3k + y_3 + h_3r &= x_6k + y_6 + h_6r, & x_1k + z_1 + (h_1 + 1)r &= x_6k + z_6 + (h_6 + 1)r, \\ x_2k + z_2 + (h_2 + 1)r &= x_4k + z_4 + (h_4 + 1)r, & x_3k + z_3 + (h_3 + 1)r &= x_5k + z_5 + (h_5 + 1)r, \\ r[r - (x_1 + 1)k + y_1] + r - (x_1 + 1)k + z_1 &= r[r - (x_5 + 1)k + y_5] + r - (x_5 + 1)k + z_5, \\ r[r - (x_2 + 1)k + y_2] + r - (x_2 + 1)k + z_2 &= r[r - (x_6 + 1)k + y_6] + r - (x_6 + 1)k + z_6, \\ r[r - (x_3 + 1)k + y_3] + r - (x_3 + 1)k + z_3 &= r[r - (x_4 + 1)k + y_4] + r - (x_4 + 1)k + z_4. \end{aligned}$$

That is,  $x_3 = x_6$ ,  $y_3 = y_6$ ,  $z_3 = z_6$  and  $h_3 = h_6$ , a contradiction to the assumption. By Theorem 2.3, we know that  $\mathcal{C}_2$  is a  $\overline{3}\text{-SC}(3, kr^2/2, r^2)$ .

In a similar fashion, we can prove that  $\mathcal{C}_3$  is also a  $\overline{3}\text{-SC}(3, kr^2/2, r^2)$ . The proof is then completed.  $\square$

As a matter of fact,  $A_1$  in Example 4.6 corresponds to  $\mathcal{C}_2$  with  $k = 2$ , while  $A_2$  corresponds to  $\mathcal{C}_3$  with  $k = 2$ .

From the constructions of  $\mathcal{C}_i$ ,  $i = 1, 2, 3$ , it can be easily checked that the following assertions hold

**Corollary 4.8.** (i)  $\mathcal{C}_i \cap \mathcal{C}_j = \emptyset$  for any distinct integers  $i, j \in \{1, 2, 3\}$ ;  
(ii) The related array of  $\mathcal{C} = \mathcal{C}_1 \cup \mathcal{C}_2 \cup \mathcal{C}_3$  is a partial Latin square;  
(iii) For any  $(a, b, c)^T \in \mathcal{C}_2$  and  $(d, e, f)^T \in \mathcal{C}_3$ , we have  $a \neq d$ ,  $b \neq e$  and  $c \neq f$ .

From Corollary 4.8, we have the following result.

**Theorem 4.9.** Let  $r = k^2$ , where  $k$  is an even positive integer. Then  $\mathcal{C} = \mathcal{C}_1 \cup \mathcal{C}_2 \cup \mathcal{C}_3$  is a  $\overline{3}\text{-SC}(3, r^3 + kr^2, r^2)$ .

**Proof:** According to Corollary 4.8 and Lemma 4.2, the related array of  $\mathcal{C}$  is a partial Latin square, and  $\mathcal{C}$  is a 2-FPC. Let

$$\begin{aligned} \alpha_i &= (a_i r + b_i, a_i r + c_i, b_i r + c_i)^T \in \mathcal{C}_1, \\ \beta_i &= (g_1(x_i, y_i, z_i, h_i), g_2(x_i, y_i, z_i, h_i), g_3(x_i, y_i, z_i, h_i))^T \in \mathcal{C}_2 \end{aligned}$$

$$\gamma_i = (g_1(x_i, y_i, z_i, h_i), g'_2(x_i, y_i, z_i, h_i), g'_3(x_i, y_i, z_i, h_i))^T \in \mathcal{C}_3,$$

where  $1 \leq i \leq 6$ . From Theorem 2.3, to prove that  $\mathcal{C}$  is a  $\overline{3}$ -SC, we only need consider the forbidden configurations in (1) and (2).

(I) Assume that  $\Delta_1 = (\mathbf{c}_1, \mathbf{c}_2, \mathbf{c}_3, \mathbf{c}_4)$  occurs in  $\mathcal{C}$ , where  $\mathbf{c}_i \in \mathcal{C}_{k_i}$  and  $k_i \in \{1, 2, 3\}$ ,  $i \in \{1, 2, 3, 4\}$ . Let us consider the 4-tuple vector  $(k_1, k_2, k_3, k_4)$ .

(1) Suppose that  $(k_1, k_2, k_3, k_4) \in K_1 = \{(k, k, k, k) \mid k \in \{1, 2, 3\}\}$ . This implies that the codewords  $\mathbf{c}_1, \mathbf{c}_2, \mathbf{c}_3, \mathbf{c}_4$  are all in the same subcode  $\mathcal{C}_k$ ,  $k \in \{1, 2, 3\}$ , a contradiction to the fact that  $\mathcal{C}_k$  is a  $\overline{3}$ -SC.

(2) Suppose that  $(k_1, k_2, k_3, k_4) \in K_2$ , where  $K_2 = \{(2, 3, k_3, k_4), (2, k_2, 3, k_4), (2, k_2, k_3, 3), (k_1, 2, k_3, 3), (k_1, k_2, 2, 3), (3, 2, k_3, k_4), (3, k_2, 2, k_4), (3, k_2, k_3, 2), (k_1, 3, k_3, 2), (k_1, k_2, 3, 2) \mid k_1, k_2, k_3, k_4 \in \{1, 2, 3\}\}$ . This contradicts the statement (iii) of Corollary 4.8.

(3) Suppose that  $(k_1, k_2, k_3, k_4) \in K_3 = \{1, 2, 3\}^4 \setminus (K_1 \cup K_2)$ . It is easy to check that none of the above cases equals  $\Delta_1$ . We take  $(k_1, k_2, k_3, k_4) = (1, 1, 1, 2)$  as an example. Suppose that  $\Delta_1 = (\alpha_1, \alpha_2, \alpha_3, \beta_4)$ . We have

$$a_1r + b_1 = a_2r + b_2, a_1r + c_1 = x_4k + z_4 + (h_4 + 1)r, b_1r + c_1 = b_3r + c_3, \\ b_2r + c_2 = [r - (x_4 + 1)k + y_4]r + [r - (x_4 + 1)k + z_4], a_3r + b_3 = x_4k + y_4 + h_4r.$$

That is,  $x_4k + y_4 = b_3 = b_1 = b_2 = r - (x_4 + 1)k + y_4$ . This implies  $2x_4 + 1 = k$ , a contradiction to the fact that  $k$  is even.

According to (1)-(3) above, we know that  $\Delta_1$  does not occur in  $\mathcal{C}$ . Similarly, we can prove that  $\Delta_2$  and  $\Delta_3$  do not occur in  $\mathcal{C}$ .

(II) Assume that  $\nabla = (\mathbf{c}_1, \mathbf{c}_2, \mathbf{c}_3, \mathbf{c}_4, \mathbf{c}_5, \mathbf{c}_6)$  occurs in  $\mathcal{C}$ , where  $\mathbf{c}_i \in \mathcal{C}_{k_i}$  and  $k_i \in \{1, 2, 3\}$ ,  $i \in \{1, 2, 3, 4, 5, 6\}$ . Let us consider the 6-tuple vector  $(k_1, k_2, k_3, k_4, k_5, k_6)$ .

(1) Suppose that  $(k_1, k_2, k_3, k_4, k_5, k_6) \in K_1 = \{(k, k, k, k, k, k) \mid k \in \{1, 2, 3\}\}$ . This implies that the codewords  $\mathbf{c}_1, \mathbf{c}_2, \mathbf{c}_3, \mathbf{c}_4, \mathbf{c}_5, \mathbf{c}_6$  are all in the same subcode  $\mathcal{C}_k$ ,  $k \in \{1, 2, 3\}$ , a contradiction to the fact that  $\mathcal{C}_k$  is a  $\overline{3}$ -SC.

(2) Suppose that  $(k_1, k_2, k_3, k_4, k_5, k_6) \in K_2$ , where  $K_2$  equals

$$\{(2, k_2, k_3, 3, k_5, k_6), (2, k_2, k_3, k_4, 3, k_6), (2, k_2, k_3, k_4, k_5, 3), (3, k_2, k_3, 2, k_5, k_6), \\ (3, k_2, k_3, k_4, 2, k_6), (3, k_2, k_3, k_4, k_5, 2), (k_1, 2, k_3, 3, k_5, k_6), (k_1, 2, k_3, k_4, 3, k_6), \\ (k_1, 2, k_3, k_4, k_5, 3), (k_1, 3, k_3, 2, k_5, k_6), (k_1, 3, k_3, k_4, 2, k_6), (k_1, 3, k_3, k_4, k_5, 2), \\ (k_1, k_2, 2, 3, k_5, k_6), (k_1, k_2, 2, k_4, 3, k_6), (k_1, k_2, 2, k_4, k_5, 3), (k_1, k_2, 3, 2, k_5, k_6), \\ (k_1, k_2, 3, k_4, 2, k_6), (k_1, k_2, 3, k_4, k_5, 2) \mid k_1, k_2, k_3, k_4, k_5, k_6 \in \{1, 2, 3\}\}.$$

This contradicts the statement (iii) of Corollary 4.8.

(3) Suppose that  $(k_1, k_2, k_3, k_4, k_5, k_6) \in K_3 = \{1, 2, 3\}^6 \setminus (K_1 \cup K_2)$ . It is easy to check that none of the above cases equals  $\nabla$ . We take  $(1, 1, 1, 1, 2, 3)$  as an example. Let  $\nabla = (\alpha_1, \alpha_2, \alpha_3, \alpha_4, \beta_5, \gamma_6)$ . We have

$$a_1r + b_1 = a_4r + b_4, \\ a_1r + c_1 = r - (x_6 + 1)k + z_6 + (h_6 + 1)r, \\ b_1r + c_1 = [r - (x_5 + 1)k + y_5]r + [r - (x_5 + 1)k + z_5], \\ a_2r + b_2 = x_5k + y_5 + h_5r, \\ a_2r + c_2 = a_4r + c_4,$$

$$\begin{aligned}
b_3r + c_3 &= [r - (x_6 + 1)k + y_6]r + x_6k + z_6, \\
a_3r + b_3 &= x_6k + y_6 + h_6r, \\
a_3r + c_3 &= x_5k + z_5 + (h_5 + 1)r, \\
b_3r + c_3 &= b_4r + c_4.
\end{aligned}$$

Then  $h_6 \equiv h_6 + 2 \pmod{r}$ , a contradiction to the fact  $r \geq 4$ .

According to (1)-(3) above, we know that  $\nabla$  does not occur in  $\mathcal{C}$ .

From the discussion above, we know that  $\mathcal{C}$  is a  $\overline{3}$ -SC, and  $|\mathcal{C}| = |\mathcal{C}_1 \cup \mathcal{C}_2 \cup \mathcal{C}_3| = |\mathcal{C}_1| + |\mathcal{C}_2| + |\mathcal{C}_3| = r^2(k + r)$ . The proof is then completed.  $\square$

**4.2. Constructions via Steiner triple systems.** In this subsection, some  $\overline{3}$ -SC(3,  $M$ ,  $q$ )s are constructed by means of Steiner triple systems, which are first used to construct partial Latin squares. Let us see its definition first.

**Definition 4.10.** Let  $v$  be a positive integer. A *Steiner triple system* (STS( $v$ ) in short) is a set system  $(V, \mathcal{B})$  where  $V$  is a set of  $v$  elements and  $\mathcal{B}$  is a set of 3-subsets of  $V$  called blocks such that every pair of distinct elements of  $V$  occurs in exactly one block of  $\mathcal{B}$ .

It is well-known that Steiner triple systems can be constructed from  $(v, 3, 1)$ -difference families. Let  $\mathcal{F}$  be a family of 3-subsets of an additive group  $G$  with order  $v$ .  $\mathcal{F}$  is called a *difference family* (briefly denoted  $(v, 3, 1)$ -DF) if any nonzero element of  $G$  can be represented in a unique way as a difference of two elements lying in some member of  $\mathcal{F}$ . Then the set system  $(G, \mathcal{B})$  is a Steiner triple system of order  $v$ , where  $\mathcal{B} = \{B + g \mid B \in \mathcal{F}, g \in G\}$ .

**Lemma 4.11.** ([14]) Let  $q = 6t + 1$  be a prime power,  $\varepsilon$  be a primitive element in  $F_q$ , and  $\xi = \varepsilon^{2t}$  be a primitive 3rd root of unity in  $F_q$ . Then  $\mathcal{F} = \{\{1, \xi, \xi^2\}\varepsilon^i \mid 0 \leq i \leq t - 1\}$  is a  $(v, 3, 1)$ -DF.

Given an STS( $v$ )  $(V, \mathcal{B})$ , we can define its corresponding partial Latin square  $\mathbb{P}$  to be the  $v \times v$ -array with entry  $k$  in cell  $(i, j)$  if and only if  $\{i, j, k\} \in \mathcal{B}$ , that is, we can derive six entries  $(x, y, z)$ ,  $(x, z, y)$ ,  $(y, x, z)$ ,  $(y, z, x)$ ,  $(z, y, x)$  and  $(z, x, y)$  in  $\mathbb{P}$  from each triple  $\{x, y, z\} \in \mathcal{B}$ .

Given a set  $S \subseteq \{0, 1, \dots, t - 1\}$ , let  $D = \{(1, \xi, \xi^2)^T \varepsilon^i \mid i \in S\}$  and  $\mathcal{C} = \{D + g \mid g \in F_q\}$ . Clearly, the related array of  $\mathcal{C}$  is a partial Latin square with  $q|S|$  non-empty cells. From Lemma 4.2, we know that  $\mathcal{C}$  is a 2-FPC(3,  $q|S|$ ,  $q$ ). Now, let us consider the forbidden configurations in (1) and (2).

(I) Without loss of generality, we may assume

$$\Delta_1 = \begin{pmatrix} \varepsilon^x & \varepsilon^y + k_1 & \varepsilon^z + k_2 & \varepsilon^w + k_3 \\ \varepsilon^x \xi & \varepsilon^y \xi + k_1 & \varepsilon^z \xi + k_2 & \varepsilon^w \xi + k_3 \\ \varepsilon^x \xi^2 & \varepsilon^y \xi^2 + k_1 & \varepsilon^z \xi^2 + k_2 & \varepsilon^w \xi^2 + k_3 \end{pmatrix},$$

where  $x, y, z, w \in S$  and  $k_1, k_2, k_3 \in F_q$ . Then we have

$$\begin{cases} \varepsilon^x = \varepsilon^y + k_1 \\ \varepsilon^z + k_2 = \varepsilon^w + k_3 \\ \varepsilon^x \xi = \varepsilon^y \xi + k_1 \\ \varepsilon^x \xi^2 = \varepsilon^z \xi^2 + k_2 \\ \varepsilon^y \xi^2 + k_1 = \varepsilon^w \xi^2 + k_3 \end{cases} \iff \begin{cases} k_1 = \varepsilon^x - \varepsilon^y \\ \varepsilon^z + \varepsilon^x \xi^2 - \varepsilon^z \xi^2 = \varepsilon^w + \varepsilon^x \xi - \varepsilon^w \xi \\ k_3 = \varepsilon^x \xi - \varepsilon^w \xi \\ k_2 = \varepsilon^x \xi^2 - \varepsilon^z \xi^2 \\ \varepsilon^y \xi^2 + \varepsilon^x - \varepsilon^y = \varepsilon^w \xi^2 + \varepsilon^x \xi - \varepsilon^w \xi \end{cases}$$

This means

$$\varepsilon^w + \varepsilon^x \xi + \varepsilon^z \xi^2 = 0 \quad \text{and} \quad \varepsilon^x + \varepsilon^w \xi + \varepsilon^y \xi^2 = 0,$$

with  $|\{x, y, z, w\}| = 4$ . In fact,

- (1)  $x \neq y, z, w$  always holds. If  $x = y$ , we have  $k_1 = \varepsilon^x - \varepsilon^y = 0$ . This implies that the first codeword equals the second codeword of  $\Delta_1$ , a contradiction to the assumption. Similarly, from  $k_2 = \varepsilon^x \xi^2 - \varepsilon^z \xi^2$  and  $k_3 = \varepsilon^x \xi - \varepsilon^w \xi$ , we have  $x \neq z, w$ .
- (2)  $y \neq z, w$  always holds. If  $y = z$ , we have  $x = w$  from  $\varepsilon^w + \varepsilon^x \xi + \varepsilon^z \xi^2 = 0$  and  $\varepsilon^x + \varepsilon^w \xi + \varepsilon^y \xi^2 = 0$ . This is a contradiction to the fact  $x \neq w$ . Similarly, from  $\varepsilon^x + \varepsilon^w \xi + \varepsilon^y \xi^2 = 0$ , we have  $y \neq w$ .
- (3)  $z \neq w$  always holds. If  $z = w$ , from  $\varepsilon^w + \varepsilon^x \xi + \varepsilon^z \xi^2 = 0$ , we have  $x = z$ , a contradiction to the fact  $x \neq z$ .

The converse can be also proved to be true.

From the discussion above, we know that  $\Delta_1$  occurs in  $\mathcal{C}$  if and only if there exists a solution to the following system of equations.

$$\begin{cases} \varepsilon^w + \varepsilon^x \xi + \varepsilon^z \xi^2 = 0 \\ \varepsilon^x + \varepsilon^w \xi + \varepsilon^y \xi^2 = 0 \\ |\{x, y, z, w\}| = 4 \end{cases}, \quad \text{where } x, y, z, w \in S. \quad (3)$$

Similarly, we can check that any of  $\Delta_2, \Delta_3$  occurs in  $\mathcal{C}$  if and only if there exists a solution to the above system of equations.

(II) Without loss of generality, we may assume

$$\nabla = \begin{pmatrix} \varepsilon^x & \varepsilon^y + k_1 & \varepsilon^z + k_2 & \varepsilon^u + k_3 & \varepsilon^v + k_4 & \varepsilon^w + k_5 \\ \varepsilon^x \xi & \varepsilon^y \xi + k_1 & \varepsilon^z \xi + k_2 & \varepsilon^u \xi + k_3 & \varepsilon^v \xi + k_4 & \varepsilon^w \xi + k_5 \\ \varepsilon^x \xi^2 & \varepsilon^y \xi^2 + k_1 & \varepsilon^z \xi^2 + k_2 & \varepsilon^u \xi^2 + k_3 & \varepsilon^v \xi^2 + k_4 & \varepsilon^w \xi^2 + k_5 \end{pmatrix},$$

where  $x, y, z, u, v, w \in S$  and  $k_1, k_2, k_3, k_4, k_5 \in F_q$ . Then we have

$$\begin{cases} \varepsilon^x = \varepsilon^u + k_3 \\ \varepsilon^y + k_1 = \varepsilon^v + k_4 \\ \varepsilon^z + k_2 = \varepsilon^w + k_5 \\ \varepsilon^x \xi = \varepsilon^w \xi + k_5 \\ \varepsilon^y \xi + k_1 = \varepsilon^u \xi + k_3 \\ \varepsilon^z \xi + k_2 = \varepsilon^v \xi + k_4 \\ \varepsilon^x \xi^2 = \varepsilon^v \xi^2 + k_4 \\ \varepsilon^y \xi^2 + k_1 = \varepsilon^w \xi^2 + k_5 \\ \varepsilon^z \xi^2 + k_2 = \varepsilon^u \xi^2 + k_3 \end{cases} \iff \begin{cases} k_3 = \varepsilon^x - \varepsilon^u \\ k_1 = \varepsilon^v + \varepsilon^x \xi^2 - \varepsilon^v \xi^2 - \varepsilon^y \\ k_2 = \varepsilon^w + \varepsilon^x \xi - \varepsilon^w \xi - \varepsilon^z \\ k_5 = \varepsilon^x \xi - \varepsilon^w \xi \\ k_1 = \varepsilon^u \xi + \varepsilon^x - \varepsilon^u - \varepsilon^y \xi \\ k_2 = \varepsilon^v \xi + \varepsilon^x \xi^2 - \varepsilon^v \xi^2 - \varepsilon^z \xi \\ k_4 = \varepsilon^x \xi^2 - \varepsilon^v \xi^2 \\ k_1 = \varepsilon^w \xi^2 + \varepsilon^x \xi - \varepsilon^w \xi - \varepsilon^y \xi^2 \\ k_2 = \varepsilon^u \xi^2 + \varepsilon^x - \varepsilon^u - \varepsilon^z \xi^2 \end{cases}.$$

This means

$$\varepsilon^x + \varepsilon^y \xi^2 + \varepsilon^z \xi = 0, \quad \varepsilon^u + \varepsilon^v \xi + \varepsilon^w \xi^2 = 0 \quad \text{and} \quad \varepsilon^x \xi + \varepsilon^u = \varepsilon^z + \varepsilon^w \xi,$$

where

$$\begin{cases} x \notin \{u, v, w\} \text{ and } |\{u, v, w\}| = 3 & \text{if } x = y = z; \\ u \notin \{x, y, z\} \text{ and } |\{x, y, z\}| = 3 & \text{if } u = v = w; \\ |\{x, y, z, u, v, w\}| = 6 & \text{otherwise.} \end{cases} \quad (4)$$

From the discussion above, we have

- (1)  $\{x, y, z\} \cap \{u, v, w\} = \emptyset$  always holds.
  - $x \notin \{u, v, w\}$  always holds. If  $x = u$ , we have  $k_3 = \varepsilon^x - \varepsilon^u = 0$ . This implies that the first codeword of  $\nabla$  equals the forth codeword of  $\nabla$ , a contradiction to the assumption. Similarly, from  $k_5 = \varepsilon^x \xi - \varepsilon^w \xi$  and  $k_4 = \varepsilon^x \xi^2 - \varepsilon^v \xi^2$ , we can prove that  $x \neq w, v$  always holds.
  - $y \notin \{u, v, w\}$  always holds. If  $y = u$ , we have  $k_1 = k_3$  from  $\varepsilon^y \xi + k_1 = \varepsilon^u \xi + k_3$ . This implies that the second codeword of  $\nabla$  equals the forth codeword of  $\nabla$ , a contradiction to the assumption. Similarly, from  $\varepsilon^y + k_1 = \varepsilon^v + k_4$  and  $\varepsilon^y \xi^2 + k_1 = \varepsilon^w \xi^2 + k_5$ , we have  $y \neq v, w$ .
  - $z \notin \{u, v, w\}$  always holds. If  $z = u$ , we have  $k_2 = k_3$  from  $\varepsilon^z \xi^2 + k_2 = \varepsilon^u \xi^2 + k_3$ . This implies that the third codeword of  $\nabla$  equals the forth codeword of  $\nabla$ , a contradiction to the assumption. Similarly, from  $\varepsilon^z + k_2 = \varepsilon^w + k_5$  and  $\varepsilon^z \xi + k_2 = \varepsilon^v \xi + k_4$ , we have  $z \neq w, v$ .
- (2) If  $|\{x, y, z\}| < 3$  (or  $|\{u, v, w\}| < 3$ ), then  $|\{x, y, z\}| = 1$  (or  $|\{u, v, w\}| = 1$ ) always holds. Without loss of generality, we may assume  $x = y$ . Then we have  $x = y = z$  from  $\varepsilon^x + \varepsilon^y \xi^2 + \varepsilon^z \xi = 0$ . Similarly, we have that if  $|\{u, v, w\}| < 3$ , then  $|\{u, v, w\}| = 1$  always holds from  $\varepsilon^u + \varepsilon^v \xi + \varepsilon^w \xi^2 = 0$ .
- (3) If  $x = y = z$  (or  $u = v = w$ ), then  $|\{u, v, w\}| = 3$  (or  $|\{x, y, z\}| = 3$ ) always holds. If  $x = y = z$  and  $u = v = w$ , we have  $\varepsilon^x = \varepsilon^u$  from  $\varepsilon^x \xi + \varepsilon^u = \varepsilon^z + \varepsilon^w \xi$ . This is a contradiction to the fact  $x \neq u$ .

The converse can be also proved to be true.

Summarizing the discussion above, we know that  $\nabla$  occurs in  $\mathcal{C}$  if and only if there exists a solution to the following system of equations.

$$\begin{cases} \varepsilon^x + \varepsilon^y \xi^2 + \varepsilon^z \xi = 0 \\ \varepsilon^u + \varepsilon^v \xi + \varepsilon^w \xi^2 = 0 \\ \varepsilon^x \xi + \varepsilon^u = \varepsilon^z + \varepsilon^w \xi \end{cases}, \text{ where } \begin{cases} x \notin \{u, v, w\} \text{ and } |\{u, v, w\}| = 3 & \text{if } x = y = z; \\ u \notin \{x, y, z\} \text{ and } |\{x, y, z\}| = 3 & \text{if } u = v = w; \\ |\{x, y, z, u, v, w\}| = 6 & \text{otherwise.} \end{cases} \quad (5)$$

Therefore we have the following result.

**Theorem 4.12.**  $\mathcal{C}$  is a  $\overline{3}\text{-SC}(3, q|S|, q)$  if and only if each solution to (3) and (5) does not belong to  $S$ .

With the aid of a computer, by applying Theorem 4.12, we obtain the following results for small  $q$ .

- Corollary 4.13.**
- (1) There exists a  $\overline{3}\text{-SC}(3, \frac{q(q-1)}{6}, q)$ , when  $q = 73, 79, 103, 127, 139$ .
  - (2) There exists a  $\overline{3}\text{-SC}(3, \lfloor \frac{q(q-1)}{9} \rfloor, q)$ , when  $q = 109, 121, 157, 169, 199, 229, 313$ .
  - (3) There exists a  $\overline{3}\text{-SC}(3, \lfloor \frac{q(q-1)}{12} \rfloor, q)$ , when  $q = 151, 157, 163, 193, 211, 223, 241, 271, 277, 283, 307, 337, 349, 367, 409, 433, 499, 523, 547, 571, 577, 601, 727, 739, 811, 859$ .
  - (4) There exists a  $\overline{3}\text{-SC}(3, \lfloor \frac{q(q-1)}{18} \rfloor, q)$ , when  $q = 181, 313, 331, 343, 373, 397, 421, 439, 457, 499, 529, 541, 607, 613, 619, 625, 673, 691, 733, 751, 757, 787, 823, 841, 877, 907, 919, 937, 961, 967, 991, 997$ .

**Proof:** The results are obtained by letting  $S = \{0, 1, \dots, t-1\}$ ,  $\{i \mid i \not\equiv 0 \pmod{3}, 0 \leq i < t\}$ ,  $\{i \mid i \equiv 0 \pmod{2}, 0 \leq i < t\}$ ,  $\{i \mid i \equiv 0 \pmod{3}, 0 \leq i < t\}$ , respectively.  $\square$

## 5. SUMMARY

In this paper, a new upper bound  $M(\overline{3}, 3, q) \leq \lfloor \frac{3q^2}{4} \rfloor$  was derived by considering an optimization problem related to a partial Latin square. Taking advantage of perfect hash families, we constructed  $\overline{3}$ -SC( $3, r^3, r^2$ )s for all positive integers  $r$ . Consequently, a lower bound  $M(\overline{3}, 3, q) \geq \lfloor \sqrt{q} \rfloor^3$  was obtained, and for every even integer  $k$ , a  $\overline{3}$ -SC( $3, r^3 + kr^2, r^2$ ) was constructed where  $r = k^2$ . Finally, the constructions of  $\overline{3}$ -SC( $3, M, q$ ) from Steiner triple systems were also discussed.

## APPENDIX: PROOF OF THEOREM 2.3

The necessity is clear from Theorem 1.3 and the discussion in Section 2. We consider its sufficiency. From the relationship between a separable code and a frameproof code in Theorem 1.3, it is sufficient to prove that for any distinct  $A, B \subseteq \mathcal{C}$  with  $|A| = |B| = 3$ , we have  $\text{desc}(A) \neq \text{desc}(B)$  except that  $A \cup B$  equals one of the forbidden configurations in (1) and (2).

Let  $A = \{\mathbf{a} = (a_1, a_2, a_3)^T, \mathbf{b} = (b_1, b_2, b_3)^T, \mathbf{c} = (c_1, c_2, c_3)^T\} \subseteq \mathcal{C}$  and  $B = \{\mathbf{d} = (d_1, d_2, d_3)^T, \mathbf{e} = (e_1, e_2, e_3)^T, \mathbf{f} = (f_1, f_2, f_3)^T\} \subseteq \mathcal{C}$ . Suppose that  $\text{desc}(A) = \text{desc}(B)$ ,  $A \neq B$  and  $|A| = |B| = 3$ . Then we have  $\{a_1, b_1, c_1\} = \{d_1, e_1, f_1\}$ ,  $\{a_2, b_2, c_2\} = \{d_2, e_2, f_2\}$  and  $\{a_3, b_3, c_3\} = \{d_3, e_3, f_3\}$  by the definition of a separable code. There are three cases to be considered:

(I)  $|A \cap B| = 2$ . Without loss of generality, we may assume that  $\mathbf{b} = \mathbf{e}$  and  $\mathbf{c} = \mathbf{f}$ , that is,  $A = \{\mathbf{a}, \mathbf{b}, \mathbf{c}\}$ ,  $B = \{\mathbf{b}, \mathbf{c}, \mathbf{d}\}$ . We list them as follows.

$$\begin{pmatrix} a_1 & b_1 & c_1 & d_1 \\ a_2 & b_2 & c_2 & d_2 \\ a_3 & b_3 & c_3 & d_3 \end{pmatrix} \quad (6)$$

Since  $\mathcal{C}$  is a 2-FPC, the following statements hold.

$\triangleright \mathbf{d} \notin \text{desc}(\{\mathbf{a}, \mathbf{b}\})$  holds because  $\mathbf{d} \notin \{\mathbf{a}, \mathbf{b}\}$ . Without loss of generality, we may assume that  $d_1 \notin \{a_1, b_1\}$ , then  $c_1 = d_1$  and  $a_1 = b_1$  always hold since  $\{a_1, b_1, c_1\} = \{b_1, c_1, d_1\}$ . Then (6) can be written as follows.

$$\begin{pmatrix} a_1 & a_1 & c_1 & c_1 \\ a_2 & b_2 & c_2 & d_2 \\ a_3 & b_3 & c_3 & d_3 \end{pmatrix} \quad (7)$$

$\triangleright \mathbf{d} \notin \text{desc}(\{\mathbf{b}, \mathbf{c}\})$  holds because  $\mathbf{d} \notin \{\mathbf{b}, \mathbf{c}\}$ . Without loss of generality, we may assume that  $d_2 \notin \{b_2, c_2\}$ , then  $a_2 = d_2$  always holds since  $\{a_2, b_2, c_2\} = \{b_2, c_2, d_2\}$ . Then (7) can be written as follows.

$$\begin{pmatrix} a_1 & a_1 & c_1 & c_1 \\ a_2 & a_2 & c_2 & d_2 \\ a_3 & b_3 & c_3 & d_3 \end{pmatrix} \quad (8)$$

$\triangleright \mathbf{d} \notin \text{desc}(\{\mathbf{a}, \mathbf{c}\})$  holds because  $\mathbf{d} \notin \{\mathbf{a}, \mathbf{c}\}$ . Then we must have  $d_3 \notin \{a_3, c_3\}$ , which implies  $b_3 = d_3$  and  $a_3 = c_3$  since  $\{a_3, b_3, c_3\} = \{b_3, c_3, d_3\}$ . Then (8) can be written as follows.

$$\begin{pmatrix} a_1 & a_1 & c_1 & c_1 \\ a_2 & b_2 & c_2 & a_2 \\ a_3 & b_3 & a_3 & b_3 \end{pmatrix} \quad (9)$$

Obviously, (9) equals  $\triangle_1$  in (1), which is a forbidden configuration in  $\mathcal{C}$ .

(II)  $|A \cap B| = 1$ . Without loss of generality, we may assume that  $\mathbf{c} = \mathbf{f}$ , that is,  $A = \{\mathbf{a}, \mathbf{b}, \mathbf{c}\}$ ,  $B = \{\mathbf{c}, \mathbf{d}, \mathbf{e}\}$ . We list them as follows.

$$\begin{pmatrix} a_1 & b_1 & c_1 & d_1 & e_1 \\ a_2 & b_2 & c_2 & d_2 & e_2 \\ a_3 & b_3 & c_3 & d_3 & e_3 \end{pmatrix} \quad (10)$$

Since  $\mathcal{C}$  is a 2-FPC, the following statements hold.

$\triangleright \mathbf{d} \notin \text{desc}(\{\mathbf{a}, \mathbf{b}\})$  holds because  $\mathbf{d} \notin \{\mathbf{a}, \mathbf{b}\}$ . Without loss of generality, we may assume that  $d_1 \notin \{a_1, b_1\}$ , then  $c_1 = d_1$  and  $a_1 = b_1 = e_1$  always hold since  $\{a_1, b_1, c_1\} = \{c_1, d_1, e_1\}$ . Then (10) can be written as follows.

$$\begin{pmatrix} a_1 & a_1 & c_1 & c_1 & a_1 \\ a_2 & b_2 & c_2 & d_2 & e_2 \\ a_3 & b_3 & c_3 & d_3 & e_3 \end{pmatrix} \quad (11)$$

$\triangleright \mathbf{e} \notin \text{desc}(\{\mathbf{a}, \mathbf{b}\})$  holds because  $\mathbf{e} \notin \{\mathbf{a}, \mathbf{b}\}$ . Without loss of generality, we may assume that  $e_2 \notin \{a_2, b_2\}$ , then  $c_2 = e_2$  and  $a_2 = b_2 = d_2$  always hold since  $\{a_2, b_2, c_2\} = \{c_2, d_2, e_2\}$ . Then (11) can be written as follows.

$$\begin{pmatrix} a_1 & a_1 & c_1 & c_1 & a_1 \\ a_2 & a_2 & c_2 & a_2 & c_2 \\ a_3 & b_3 & c_3 & d_3 & e_3 \end{pmatrix} \quad (12)$$

$\triangleright \mathbf{d} \notin \text{desc}(\{\mathbf{b}, \mathbf{c}\})$  holds because  $\mathbf{d} \notin \{\mathbf{b}, \mathbf{c}\}$ . Then we must have  $d_3 \notin \{b_3, c_3\}$ , which implies  $a_3 = d_3$  since  $\{a_3, b_3, c_3\} = \{c_3, d_3, e_3\}$ . Then (12) can be written as follows.

$$\begin{pmatrix} a_1 & a_1 & c_1 & c_1 & a_1 \\ a_2 & a_2 & c_2 & a_2 & c_2 \\ a_3 & b_3 & c_3 & a_3 & e_3 \end{pmatrix}$$

Obviously,  $\mathbf{d} \in \text{desc}(\{\mathbf{a}, \mathbf{c}\})$  holds. This contradicts the definition of a 2-FPC since  $\mathbf{d} \notin \{\mathbf{a}, \mathbf{c}\}$ .

So the case of  $|A \cap B| = 1$  can never happen.

(III)  $|A \cap B| = 0$ . We list  $A$  and  $B$  as follows.

$$\begin{pmatrix} a_1 & b_1 & c_1 & d_1 & e_1 & f_1 \\ a_2 & b_2 & c_2 & d_2 & e_2 & f_2 \\ a_3 & b_3 & c_3 & d_3 & e_3 & f_3 \end{pmatrix} \quad (13)$$

Since  $\mathcal{C}$  is a 2-FPC, the following statements hold.



$\triangleright \mathbf{d} \notin \text{desc}(\{\mathbf{a}, \mathbf{b}\})$  holds because  $\mathbf{d} \notin \{\mathbf{a}, \mathbf{b}\}$ . Without loss of generality, we may assume that  $d_1 \notin \{a_1, b_1\}$ , then  $c_1 = d_1$  always holds since  $\{a_1, b_1, c_1\} = \{d_1, e_1, f_1\}$ . Then (13) can be written as follows.

$$\begin{pmatrix} a_1 & b_1 & c_1 & c_1 & e_1 & f_1 \\ a_2 & b_2 & c_2 & d_2 & e_2 & f_2 \\ a_3 & b_3 & c_3 & d_3 & e_3 & f_3 \end{pmatrix} \quad (14)$$

$\triangleright \mathbf{d} \notin \text{desc}(\{\mathbf{a}, \mathbf{c}\})$  holds because  $\mathbf{d} \notin \{\mathbf{a}, \mathbf{c}\}$ . Without loss of generality, we may assume that  $d_2 \notin \{a_2, c_2\}$ , then  $b_2 = d_2$  always holds since  $\{a_2, b_2, c_2\} = \{d_2, e_2, f_2\}$ . Then (14) can be written as follows.

$$\begin{pmatrix} a_1 & b_1 & c_1 & c_1 & e_1 & f_1 \\ a_2 & b_2 & c_2 & b_2 & e_2 & f_2 \\ a_3 & b_3 & c_3 & d_3 & e_3 & f_3 \end{pmatrix} \quad (15)$$

$\triangleright \mathbf{d} \notin \text{desc}(\{\mathbf{b}, \mathbf{c}\})$  holds because  $\mathbf{d} \notin \{\mathbf{b}, \mathbf{c}\}$ . Then we must have  $d_3 \notin \{b_3, c_3\}$ , which implies  $a_3 = d_3$  since  $\{a_3, b_3, c_3\} = \{d_3, e_3, f_3\}$ . Then (15) can be written as follows.

$$\begin{pmatrix} a_1 & b_1 & c_1 & c_1 & e_1 & f_1 \\ a_2 & b_2 & c_2 & b_2 & e_2 & f_2 \\ a_3 & b_3 & c_3 & a_3 & e_3 & f_3 \end{pmatrix}$$

$\triangleright \mathbf{e} \notin \text{desc}(\{\mathbf{a}, \mathbf{b}\})$  holds because  $\mathbf{e} \notin \{\mathbf{a}, \mathbf{b}\}$ . There must exist an index  $1 \leq i \leq 3$  such that  $e_i \notin \{a_i, b_i\}$  holds.

(1.1) If  $e_1 \notin \{a_1, b_1\}$  holds, then  $c_1 = e_1$  always holds since  $\{a_1, b_1, c_1\} = \{c_1, e_1, f_1\}$ ;

(1.2) If  $e_2 \notin \{a_2, b_2\}$  holds, then  $c_2 = e_2$  always holds since  $\{a_2, b_2, c_2\} = \{b_2, e_2, f_2\}$ ;

(1.3) If  $e_3 \notin \{a_3, b_3\}$  holds, then  $c_3 = e_3$  always holds since  $\{a_3, b_3, c_3\} = \{a_3, e_3, f_3\}$ .

$\triangleright \mathbf{e} \notin \text{desc}(\{\mathbf{a}, \mathbf{c}\})$  holds because  $\mathbf{e} \notin \{\mathbf{a}, \mathbf{c}\}$ . There must exist an integer  $1 \leq i \leq 3$  such that  $e_i \notin \{a_i, c_i\}$  holds.

(2.1) If  $e_1 \notin \{a_1, c_1\}$  holds, then  $b_1 = e_1$  always holds since  $\{a_1, b_1, c_1\} = \{c_1, e_1, f_1\}$ ;

(2.2) If  $e_2 \notin \{a_2, c_2\}$  holds, then  $b_2 = e_2$  always holds since  $\{a_2, b_2, c_2\} = \{b_2, e_2, f_2\}$ ;

(2.3) If  $e_3 \notin \{a_3, c_3\}$  holds, then  $b_3 = e_3$  always holds since  $\{a_3, b_3, c_3\} = \{a_3, e_3, f_3\}$ .

$\triangleright \mathbf{e} \notin \text{desc}(\{\mathbf{b}, \mathbf{c}\})$  holds because  $\mathbf{e} \notin \{\mathbf{b}, \mathbf{c}\}$ . There must exist an index  $1 \leq i \leq 3$  such that  $e_i \notin \{b_i, c_i\}$  holds.

(3.1) If  $e_1 \notin \{b_1, c_1\}$  holds, then  $a_1 = e_1$  always holds since  $\{a_1, b_1, c_1\} = \{c_1, e_1, f_1\}$ ;

(3.2) If  $e_2 \notin \{b_2, c_2\}$  holds, then  $a_2 = e_2$  always holds since  $\{a_2, b_2, c_2\} = \{b_2, e_2, f_2\}$ ;

(3.3) If  $e_3 \notin \{b_3, c_3\}$  holds, then  $a_3 = e_3$  always holds since  $\{a_3, b_3, c_3\} = \{a_3, e_3, f_3\}$ .

$\triangleright \mathbf{f} \notin \text{desc}(\{\mathbf{a}, \mathbf{b}\})$  holds because  $\mathbf{f} \notin \{\mathbf{a}, \mathbf{b}\}$ . There must exist an index  $1 \leq i \leq 3$  such that  $f_i \notin \{a_i, b_i\}$  holds.

(4.1) If  $f_1 \notin \{a_1, b_1\}$  holds, then  $c_1 = f_1$  always holds since  $\{a_1, b_1, c_1\} = \{c_1, e_1, f_1\}$ ;

(4.2) If  $f_2 \notin \{a_2, b_2\}$  holds, then  $c_2 = f_2$  always holds since  $\{a_2, b_2, c_2\} = \{b_2, e_2, f_2\}$ ;

(4.3) If  $f_3 \notin \{a_3, b_3\}$  holds, then  $c_3 = f_3$  always holds since  $\{a_3, b_3, c_3\} = \{a_3, e_3, f_3\}$ .

$\triangleright \mathbf{f} \notin \text{desc}(\{\mathbf{a}, \mathbf{c}\})$  holds because  $\mathbf{f} \notin \{\mathbf{a}, \mathbf{c}\}$ . There must exist an index  $1 \leq i \leq 3$  such that  $f_i \notin \{a_i, c_i\}$  holds.

(5.1) If  $f_1 \notin \{a_1, c_1\}$  holds, then  $b_1 = f_1$  always holds since  $\{a_1, b_1, c_1\} = \{c_1, e_1, f_1\}$ ;

(5.2) If  $f_2 \notin \{a_2, c_2\}$  holds, then  $b_2 = f_2$  always holds since  $\{a_2, b_2, c_2\} = \{b_2, e_2, f_2\}$ ;  
 (5.3) If  $f_3 \notin \{a_3, c_3\}$  holds, then  $b_3 = f_3$  always holds since  $\{a_3, b_3, c_3\} = \{a_3, e_3, f_3\}$ .  
 $\triangleright \mathbf{f} \notin \text{desc}(\{\mathbf{b}, \mathbf{c}\})$  holds because  $\mathbf{f} \notin \{\mathbf{b}, \mathbf{c}\}$ . There must exist an index  $1 \leq i \leq 3$  such that  $f_i \notin \{b_i, c_i\}$  holds.

(6.1) If  $f_1 \notin \{b_1, c_1\}$  holds, then  $a_1 = f_1$  always holds since  $\{a_1, b_1, c_1\} = \{c_1, e_1, f_1\}$ ;

(6.2) If  $f_2 \notin \{b_2, c_2\}$  holds, then  $a_2 = f_2$  always holds since  $\{a_2, b_2, c_2\} = \{b_2, e_2, f_2\}$ ;

(6.3) If  $f_3 \notin \{b_3, c_3\}$  holds, then  $a_3 = f_3$  always holds since  $\{a_3, b_3, c_3\} = \{a_3, e_3, f_3\}$ .

It is easy to check that for any  $i \in \{1, 2, 3\}$  or any  $i \in \{4, 5, 6\}$ , and for any  $j \in \{1, 2, 3\}$ , once  $(i, j)$  occurs, no  $(i', j)$  can occur for any  $i' \in \{1, 2, 3\} \setminus \{i\}$  or any  $i' \in \{4, 5, 6\} \setminus \{i\}$ , respectively. So there are  $3 \times 2 \times 1 \times 3 \times 2 \times 1 = 36$  cases to be considered.

$\{(1.3), (2.2), (3.1), (4.2), (5.1), (6.3)\}, \quad \{(1.1), (2.3), (3.2), (4.2), (5.1), (6.3)\},$   
 $\{(1.1), (2.3), (3.2), (4.2), (5.3), (6.1)\}, \quad \{(1.1), (2.3), (3.2), (4.3), (5.1), (6.2)\},$   
 $\{(1.1), (2.3), (3.2), (4.3), (5.2), (6.1)\}, \quad \{(1.2), (2.1), (3.3), (4.1), (5.3), (6.2)\},$   
 $\{(1.2), (2.1), (3.3), (4.2), (5.3), (6.1)\}, \quad \{(1.2), (2.1), (3.3), (4.3), (5.1), (6.2)\},$   
 $\{(1.2), (2.1), (3.3), (4.3), (5.2), (6.1)\}, \quad \{(1.2), (2.3), (3.1), (4.1), (5.3), (6.2)\},$   
 $\{(1.2), (2.3), (3.1), (4.2), (5.1), (6.3)\}, \quad \{(1.2), (2.3), (3.1), (4.3), (5.2), (6.1)\},$   
 $\{(1.3), (2.1), (3.2), (4.1), (5.3), (6.2)\}, \quad \{(1.3), (2.1), (3.2), (4.2), (5.1), (6.3)\},$   
 $\{(1.3), (2.1), (3.2), (4.3), (5.2), (6.1)\}, \quad \{(1.3), (2.2), (3.1), (4.1), (5.3), (6.2)\},$   
 $\{(1.3), (2.2), (3.1), (4.2), (5.3), (6.1)\}, \quad \{(1.3), (2.2), (3.1), (4.3), (5.1), (6.2)\},$   
 $\{(1.1), (2.2), (3.3), (4.1), (5.2), (6.3)\}, \quad \{(1.1), (2.2), (3.3), (4.1), (5.3), (6.2)\},$   
 $\{(1.1), (2.2), (3.3), (4.2), (5.1), (6.3)\}, \quad \{(1.1), (2.2), (3.3), (4.2), (5.3), (6.1)\},$   
 $\{(1.1), (2.2), (3.3), (4.3), (5.1), (6.2)\}, \quad \{(1.1), (2.2), (3.3), (4.3), (5.2), (6.1)\},$   
 $\{(1.1), (2.3), (3.2), (4.1), (5.2), (6.3)\}, \quad \{(1.1), (2.3), (3.2), (4.1), (5.3), (6.2)\},$   
 $\{(1.2), (2.1), (3.3), (4.1), (5.2), (6.3)\}, \quad \{(1.2), (2.1), (3.3), (4.2), (5.1), (6.3)\},$   
 $\{(1.2), (2.3), (3.1), (4.1), (5.2), (6.3)\}, \quad \{(1.2), (2.3), (3.1), (4.2), (5.3), (6.1)\},$   
 $\{(1.3), (2.1), (3.2), (4.1), (5.2), (6.3)\}, \quad \{(1.3), (2.1), (3.2), (4.3), (5.1), (6.2)\},$   
 $\{(1.3), (2.2), (3.1), (4.1), (5.2), (6.3)\}, \quad \{(1.3), (2.2), (3.1), (4.3), (5.2), (6.1)\},$   
 $\{(1.2), (2.3), (3.1), (4.3), (5.1), (6.2)\}, \quad \{(1.3), (2.1), (3.2), (4.2), (5.3), (6.1)\}.$

It is readily checked that none of the first 18 subcases satisfies the condition (i) in this theorem. For example, consider the subcase  $\{(1.3), (2.2), (3.1), (4.2), (5.1), (6.3)\}$ , that is,

$$(1.3) \ c_3 = e_3; \ (2.2) \ b_2 = e_2; \ (3.1) \ a_1 = e_1; \ (4.2) \ c_2 = f_2; \ (5.1) \ b_1 = f_1; \ (6.3) \ a_3 = f_3.$$

Then the corresponding subcode can be written as follows.

$$\begin{pmatrix} a_1 & b_1 & c_1 & c_1 & a_1 & b_1 \\ a_2 & b_2 & c_2 & b_2 & b_2 & c_2 \\ a_3 & b_3 & c_3 & a_3 & c_3 & a_3 \end{pmatrix}$$

where  $\mathbf{e} = (a_1, b_2, c_3)^T$  and  $\mathbf{f} = (b_1, c_2, a_3)^T$ . Obviously,  $\mathbf{b} \in \text{desc}(\{\mathbf{e}, \mathbf{f}\})$  holds since  $b_3 \in \{a_3, c_3\}$ . This is a contradiction to the definition of a 2-FPC because of the assumption  $\mathbf{b} \notin \{\mathbf{e}, \mathbf{f}\}$ . It is also easy to check that none of the next 16 subcases satisfies the condition that  $|B| = 3$ . Finally the remaining 2 subcases correspond to the forbidden configuration in (2).

The proof is then completed.  $\square$

## REFERENCES

- [1] M. Bazrafshan and Tran van Trung, On optimal bounds for separating hash families, Germany-Africa workshop on Information and Communication Technology, Essen, Germany, (2008).
- [2] S. R. Blackburn, Frameproof codes, SIAM J. Discrete Math. **16**, 499-510, (2003).
- [3] S. R. Blackburn, Perfect hash families: probabilistic methods and explicit constructions, J. Combin. Theory, Ser. A **92**, 54-60, (2000).
- [4] S. R. Blackburn, Probabilistic existence results for separable codes, preprint, (2015).
- [5] D. Boneh and J. Shaw, Collusion-secure fingerprinting for digital data, IEEE Trans. Inf. Theory **44**, 1897-1905, (1998).
- [6] M. Cheng, H-L. Fu, J. Jiang, Y-H. Lo and Y. Miao, New bounds on  $\overline{2}$ -separable codes of length 2, Des. Codes Cryptogr. **74**, 31-40, (2015).
- [7] M. Cheng, L. Ji and Y. Miao, Separable codes, IEEE Trans. Inf. Theory **58**, 1791- 1803, (2012).
- [8] M. Cheng and Y. Miao, On anti-collusion codes and detection algorithms for multimedia fingerprinting, IEEE Trans. Inf. Theory **57**, 4843-4851, (2011).
- [9] H. D. L. Hollmann, J. H. Lint, J.-P. Linnartz and L. M. G. M. Tolhuizen, On codes with the identifiable parent property, J. Combin. Theory, Ser. A **82**, 121-133, (1998).
- [10] J. N. Staddon, D. R. Stinson and R. Wei, Combinatorial properties of frameproof and traceability codes, IEEE Trans. Inf. Theory **47**, 1042-1049, (2001).
- [11] D. R. Stinson, Tran van Trung and R. Wei, Secure frameproof codes, key distribution patterns, group testing algorithms and related structures, J. Stat. Plan. Inference **86**, 595-617, (2000).
- [12] D. R. Stinson, R. Wei and K. Chen, On generalized separating hash families, J. Combin. Theory, Ser. A **115**, 105-120, (2008).
- [13] W. Trappe, M. Wu, Z. J. Wang and K. J. R. Liu, Anti-collusion fingerprinting for multimedia, IEEE Trans. Signal Processing **51**, 1069-1087, (2003).
- [14] R. M. Wilson, Cyclotomy and difference families in elementary abelian groups, J. Number Theory **4**, 17-47, (1972).

MINQUAN CHENG: INFORMATION SECURITY AND NATIONAL COMPUTING GRID LABORATORY, SOUTHWEST JIAOTONG UNIVERSITY, CHENGDU 610031, CHINA

*E-mail address:* chengqinshi@hotmail.com

JING JIANG: SCHOOL OF COMPUTER SCIENCE AND INFORMATION TECHNOLOGY, GUANGXI NORMAL UNIVERSITY, GUILIN 541004, CHINA

*E-mail address:* jjjiang2008@hotmail.com

HAIYAN LI: SCHOOL OF MATHEMATICS AND STATISTICS, GUANGXI NORMAL UNIVERSITY, GUILIN 541004, CHINA

*E-mail address:* lhyqw2015@sina.com

YING MIAO: FACULTY OF ENGINEERING, INFORMATION AND SYSTEMS, UNIVERSITY OF TSUKUBA, TSUKUBA, IBARAKI 305-8573, JAPAN

*E-mail address:* miao@sk.tsukuba.ac.jp

XIAOHU TANG: INFORMATION SECURITY AND NATIONAL COMPUTING GRID LABORATORY, SOUTHWEST JIAOTONG UNIVERSITY, CHENGDU 610031, CHINA

*E-mail address:* xhutang@home.swjtu.edu.cn